Journal of Civil & Legal Sciences
ISSN: 2169-0170
Mini Review Open Access

Conceptual Protection Security for Macro Corporates, Individuals and Sme's

Richard K*
Department of Law, Professor, University of Leeds, United Kingdom

Abstract

There is a widespread misconception that only huge organizations require cyber security because they run the danger of cyber-attacks and data breaches. We erroneously believe that because we are merely low profile individuals or modestly sized businesses, we are protected. This is totally untrue because everybody with internet access is vulnerable to a cyber-attack. Whether large, medium, or small, all organizations and businesses are susceptible to cyber dangers. In Nigeria Cyber security is covered majorly by the Cybercrimes Act 20152 and NITDA regulations.

Keywords: Safeguarding; System infiltrate; Vulnerable access; Ransom ware; Trustworthy party; Start-up development

Introduction

The concept of cyber security involves safeguarding your electronic systems, including computers, mobile devices, and laptops, against cyber-attacks. Cyber-attacks happen every 39 seconds and 95% of all cyber-security breaches are as a result of human error4. Every person and company should have a strong understanding of cyber security because it prevents one from falling victim to cyber criminals. Cybercriminals commit cyber-crimes that result in property loss or damage via hacking, typo-squatting or virus transmission, etc. A report by Norton revealed just how vulnerable many people are and unaware of it. According to the report, 44% of those surveyed thought themselves "worthwhile targets" for hackers. Despite these assumptions, nearly 86% of respondents thought they had experienced a phishing attack. About 40% of respondents could not definitively tell a phishing email apart from a legitimate one [1]. Cybercriminals employ diversionary tactics to infiltrate your system and one of them is password attacks. Simply put, password attacks are attempts by hackers to obtain your passwords. Some common forms of password attacks include Dictionary attack, Brute force attack, key loggers, malware, rainbow table attack and phishing.

Discussion

Phishing, a social engineering tool is the most common form of password attacks and data breaches. Phishing is when a hacker or cyber-criminal poses as a trustworthy party sends you a malicious email or message, hoping you would voluntarily divulge your personal information, including your bank account details and passwords. They frequently direct you to fake "reset your password" pages where they steal your passwords. Other times, they lead you to click on URLs that harm your system by installing malicious codes. Voice calls are also used in phishing attacks. Victims receive phone calls from cybercriminals posing often times as their financial institutions in an effort to obtain sensitive information from the unsuspecting individuals [2]. When phishing occurs in this form, it is called Phishing. Also cyber criminals can use botnets to send out massive amounts of spam, or engage in wide-scale distributed denial of service (DDoS) attacks. The 2016 DDoS attack that shut down the internet for millions of people in the United States was possible because of a massive botnet consisting of 100,000 infected devices.

Ways individuals can protect against password attacks

- Protect your phones and accounts by using multi-factor authentication to add an extra layer of security.
- Don't use the same password for multiple accounts
- Monitor your accounts and check if your email address is linked to any recent leaks.
- Install security software on your devices and set them to update automatically to provide protection against new threats.
- Avoid divulging your personal financial information in response to unsolicited request, whether over the phone or via the internet.

Cybercriminals often target small businesses, infecting their websites, and disseminating malicious malware to visitors or web users who view or interact with the site. 43% of cyber-attacks are aimed at small businesses, but only 14% are prepared to defend themselves. Because these organisations are not prepared, and since they lack funding as long-standing companies, 60% of them close within six months of a cyber-attack. Without an essential cyber-security strategy, your working environment becomes vulnerable to malicious actors which pose not only a risk to the acquisition and integrity of your data but also to your business reputation [3].

To circumvent perimeter network security, attackers frequently target employees, who pose the weakest link in cyber-security, with basic insider knowledge obtained primarily through the internet.

In the age of digitalisation and exponential data growth and accumulation, setting up a cyber-security framework is no longer a fanciful recommendation but a necessity. Not only are the regulatory requirements becoming more stringent, but consumers now expect a certain level of data protection. In fact, most prospective clients/partnerships now require organisations, regardless of size, to prove their security posture via issued Security Assessment Questionnaires (SAQ's) - a tedious survey of the policies and procedures implemented to protect data [4].

It is therefore imperative that small scale businesses understand the

***Corresponding author:** Richard K, Department of Law, Professor, University of Leeds, United Kingdom, Tel: +1642342392, E-mail: a.tammer-neisingh@uu.nl

Received: 03-Mar-2023, Manuscript No. JCLS-23-91388; **Editor assigned:** 06-Mar-2023, PreQC No. JCLS-23-91388; **Reviewed:** 20-Mar-2023, QC No. JCLS-23-91388; **Revised:** 24-Mar-2023, Manuscript No. JCLS-23-91388; **Published:** 31-Mar-2023, DOI: 10.4172/2169-0170.1000383

Citation: Richard K (2023) Conceptual Protection Security for Macro Corporates, Individuals and Sme's. J Civil Legal Sci 12: 383.

dangers of cyber-attacks and why they should prioritise cyber-security.

Here are some top reasons why SMEs should prioritise cyber-security:

SMEs are more likely to be targeted by cyber-attackers because they typically have fewer security resources than enterprise organisations.

A data breach can cause significant financial damage, ransom costs for ransom ware attacks often run into millions which may be irrecoverable at that phase of start-up development [5].

A cyber-attack can be lethal to an adolescent start-up's reputation. Consumers may be understandably wary of frequenting businesses that have been hit by attacks. Similarly, investors may view being a cyber-attack victim as a form of carelessness and may not want to involve themselves.

Cyber-security can act as a persuasive competitive differentiator amongst peers less likely to have an established program

Ways SMEs can prevent cyber-attacks

➢ Do background checks on employees: Data suggests that 43% of data breaches involve internal actors, including employees, contractors, and third-party suppliers. It's estimated that half of all data breaches that involve internal actors are intentional, while the other half are accidental.

Educate employees about the risk of cyber-attacks: Hackers and cybercriminals often penetrate systems by tricking your employees into giving them the keys. It's crucial to continually train employees on cyber-attack risks and the importance of staying vigilant [6]. Consider training sessions to show employees how to spot infected computers and suspicious emails and websites.

- ➢ Keep your wireless network secure
- ➢ Set up an automatic software update
- ➢ Apart from ensuring adequate Cyber-security measures, companies need cyber or experienced tech lawyers for the purposes of:

a. Rendering detailed advisory services on the provisions of all Cybercrime, Cyber-security & Tech legislation.

b. Ensuring regulatory compliance especially in the area of rendering Data Protection Regulations compliance returns.

c. Having experienced and diligent legal input in the drafting and documentation of IT policies , Terms and Conditions agreements, Data Protection & Password policies, as well as IT Service Level Agreements & Non-Disclosure Agreements (NDAs).

So, there would be a very bright scope for people who work and resolve the issues related to cyber-crime and provide all the necessary security measures. Big organizations like CISCO which is completely related to networking technology which is one of the top organization has approximately millions of openings related to cyber-security because which is the future for the safety of Information technology [7]. They are also wide opportunities in government-related fields and also defense field to save the countries secure data from cyber attackers. Cyber-security is both about the insecurity made by and through this new space and about the practices or procedures to make it secure. Exertion to verify the cyberspace should give a definitive need else the information technology" will not be viably used by clients [8]. The terrorist of things to come will win the wars without discharging a shot just by crushing the country's necessary substructure if steps are not taken to handle the pervasiveness of the expansion in such a cyber-attack. They can bring an unknown look into the lives of others, regardless of whether they live nearby or over the globe [9]. The cyber-terrorism can in one method or alternate prompts the death toll just as causing severe harms. Though social media can utilize for cybercrimes, these organizations cannot stand to quit utilizing social media as it assumes an essential role in the attention of an organization. Cyber terrorism has guaranteed numerous innocent lives and in the meantime renders numerous homes to a condition of the problem that is occasionally coming about to mental injury to the influenced families. Cyber terrorism stays vital issues of the present society. Not just that the battle against Cyber terrorism is falling behind, current cybercrime assaults are ending up progressively forceful and confrontational. Cyber-security has an intriguing parallel to terrorism. Guaranteeing the security of information, data, and correspondence is impressively harder than hacking into a system [10].

Conclusion

Cyber-security is everyone's responsibility as cyber threats and attacks affect everyone and every organization/ business whether large, medium or small. The goal of cyber-security is to ensure the confidentiality, integrity and availability of data in order to avoid unauthorized disclosure. Hence, as a digital citizen, it is very important to understand cyber-security and be aware of cyber safety measures.

Acknowledgement

None

Conflict of Interest

None

References

1. Yoram J, Didier T, Olivier B (2002) A satellite view of aerosols in the climate system. Nature UK 419:215-223.
2. Ramanathan P, Crutzen, J, Rosenfeld D (2001) Aerosols, climate, and the hydrological cycle. Nature UK 294:2119-24 .
3. Hassan A, Qadri MA, Saleem M (2021) The Muslim Family Law Ordinance 1961: Pioneer of Women Empowerment in Pakistan. JRSP PAK 58:1-8.
4. Abdullah R, Monsoor T, Johari F (2015) Financial support for women under Islamic family law in Bangladesh and Malaysia. Taylor and Francis UK 21:363-383.
5. Elias T (2015) Gaps and Challenges in the Enforcement Framework for Consumer Protection in Ethiopia. Miz L Rev EA 9:1-25.
6. Levitus S, John I, Wang J, Thomas L, Keith W, et al. (2001) Anthropogenic Warming of Earth's Climate System. USA 292:267-270.
7. Roger A, Jimmy A, Thomas N, Curtis H, Matsui T, et al. (2007) A new paradigm for assessing the role of agriculture in the climate system and in climate change. Agric For Meteorol EU 142:234-254.
8. Shahid TN (2013) Islam and women in the constitution of Bangladesh: The impact on family laws for Muslim women. FLJS UK 1-11.
9. Shehabuddin E (2008) Reshaping the holy: Democracy, development, and Muslim women in Bangladesh. CUP NY: 1-304.
10. Hossain K (2003) In Search of Equality: Marriage Related Laws for Muslim Women in Bangladesh.J Int Women's Stud MA 5:1-38.